UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/602,754	06/24/2003	Larry Cecil Brown	PU030107	9976

24498 7590 01/10/2011
Robert D. Shedd, Patent Operations
THOMSON Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

EXAMINER	
TOLENTINO, RODERICK	
ART UNIT	PAPER NUMBER
2439	
MAIL DATE	DELIVERY MODE
01/10/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte LARRY CECIL BROWN, MARK RYAN MAYERNICK,
SIMON ANDRE LAVAUD, and DAVID LEE RYAN

Appeal 2009-006765
Application 10/602,754
Technology Center 2400

Before JOHN C. MARTIN, MAHSHID D. SAADAT,
and ROBERT E. NAPPI, *Administrative Patent Judges*.

MARTIN, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1-19, which are all of the pending claims.

We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

A. Appellants' invention

Appellants' invention relates to a method and system for customizing a broadband access device configuration file to provide security for a service provider and/or service features for the end user. Specification 1:7-10.

On many broadband access products, such as a Data Over Cable Service Interface Specification (DOCSIS) Cable Modem, valuable troubleshooting diagnostic information elements are made available to the end user by means of an HTTP server built into the device (*id.* at 1:14-17). This built-in server enables the end user to view, using a personal computer, web pages containing this diagnostic information (*id.* at 1:17-18). Appellants' invention enables the Service Provider, from its location, to remotely configure an in-home device to reveal information elements needed to provide a service or protect the service provider's system while still limiting access to additional information (*id.* at 1:22-25).

B. The claims

The independent claims before us are claims 1 and 10, of which claim 1 reads:

> 1. A security system for use in a distributed network, comprising:
>
> a service provider selectively accessible via a network by a plurality of end users each having an access device for accessing the network; and
>
> a control mechanism disposed at a location of the service provider which accesses and modifies stored information on each access device of the end users to designate service provider-accessible portions of the information to prevent access thereof by the end users.

Claims App. (Br. 12).[2]

We do not understand the phrase "service provider-accessible portions of the information" in claim 1 to be referring to information portions that are accessible by only the service provider. Instead, this quoted claim language is broad enough to read on information portions that are initially accessible by the service provider and the end users. As a result, the claim is broad enough to permit the recited control mechanism to access and modify stored information on each access device of the end users in order to designate, as user-inaccessible, other information portions that were initially accessible by the service provider and the end users. Independent claim 10 is similarly broad.

[2] Appeal Brief filed April 3, 2008.

C. The rejections

Claims 1-8, 10, and 12-19 stand rejected under 35 U.S.C. § 102(b) for anticipation by McMullan (US 5,654,746). Final Action 2, para. 2.

Claims 9 and 11 stand rejected under 35 U.S.C. § 103(a) for obviousness over McMullan. *Id.* at 3, para. 3.

THE MERITS OF THE REJECTIONS

McMullan's invention relates to authorization and control of game delivery services. McMullan, col. 1, ll. 6-8. McMullan's invention employs first and second authorization modes in the form of a rental mode and an arcade mode, respectively (col. 2, ll. 46-48). The home communications terminal in the rental mode comprises a game adapter and in the arcade mode comprises a game player (col. 2, ll. 48-50). Authorization data and game data are transmitted periodically from a transmitter toward the home communications terminal, which provides only limited access to game data by the game player (col. 2, ll. 50-54).

Initially, the Examiner found that "[c]onfiguration information in the access device, which collectively constitutes a configuration file, may be modified using commands from the server (see column 17, lines 38-56). Though only writing from the server is disclosed by McMullan, this constitutes 'service-provider access.' The configuration file cannot be read by the user." Final Action 2. In the Answer, the Examiner more specifically finds that

> McMullan discloses the disabling of hardware in a user system (see column 17, line 52) and the designation of service provider accessible data that is inaccessible to the user (e.g. keys, passwords, see column 52 [*sic*; 17], lines 54-56). This constitutes the designation of "service provide[r] accessible portions," insofar as that term is defined in Appellant's specification.

(Answer 4-5.) The column 17 paragraph that contains the above-cited lines reads as follows:

> Another addressed transaction per FIG. 8 is the adapter control transaction which can disable a particular adapter, for example, for non-payment of subscriber bills and the like. The adapter control transaction further may be optionally utilized to change security keys, reset the adapter or reset parental passwords from the control center.

Col. 17, ll. 51-56. Regarding the disabling feature, the Examiner further explains that "McMullan's commands change the status of areas on the client such that they are service-provider accessible but disabled with respect to the client (due to non-payment of subscriber bills, for example)." January 2, 2008, Advisory Action 2.

We understand the Examiner's position to be that the claim language at issue reads on McMullan when any of the following actions are taken by the service provider: (1) disabling the hardware (e.g., for non-payment); (2) changing the security key; and (3) resetting a parental password. We will address (2) and (3) before addressing (1). We agree with Appellants (Reply Br. 5) that the Examiner's reliance on the control center's changing of a security key is misplaced. Although the security key constitutes service-provider accessible information, changing the security key does not designate it as inaccessible to the user. As correctly noted by Appellants, the security key is never accessible to the user (*id.*). As for resetting a parental password, it is not apparent -- and the Examiner has not explained -- how resetting this password satisfies the claim language.[3]

However, we are not persuaded that the Examiner erred in reading claim 1 on the issuance of a control transaction by the control center to disable the user's hardware (e.g., for non-payment). Such a control transaction presumably causes a stored information item in the adapter to be modified to indicate the hardware's disabled status, which has the effect of designating other information stored in the adapter (including at least some service-provider accessible portions) as inaccessible to the user.[4] We therefore sustain the rejection of claim 1 and the rejection of independent claim 10, as to which Appellants essentially repeat their claim 1 arguments. For the same reasons, we sustain the rejections of dependent claims 2-9 and 11-19, whose merits are not separately argued. *In re Nielson*, 816 F.2d 1567, 1572 (Fed. Cir. 1987).

DECISION

[3] It is therefore not necessary to decide whether Appellants are correct to argue that "resetting a parental passwords removes the password altogether, thereby enabling user-access of information, rather than designating the information to prevent user-access thereof." (Reply Br. 5.)

[4] Consequently, we do not agree with Appellants argument that "[d]isabling a device does not in any way label information stored on the device" (Br. 8).

The Examiner's decision that claims 1-19 are unpatentable is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1). *See* 37 C.F.R. § 1.136(a)(1)(v) (2010).

AFFIRMED

ELD

ROBERT D. SHEDD, PATENT OPERATIONS
THOMSON LICENSING LLC
P.O. BOX 5312
PRINCETON, NJ 08543-5312